



# DATA ASSURED



## Cyber Do's & Don'ts

In Partnership With:



Presented By:





## DO'S:



## DON'TS:



Use unique complex passphrases and change them regularly



Open attachments or click links from unknown sources



Turn on encryption on all devices



Use free public WiFi without a VPN



Regularly backup all your data with version controlled backups



Share passphrases or use the same phrase for multiple accounts



Use antivirus/antimalware on all devices



Scan random QR codes or accept random Airdrops



Keep all software and OS's up to date



Install apps or software from unknown sources



Pay attention to possible signs of phishing



Recycle old devices without properly wiping all data



Educate all employees



Log into any personal accounts on public computers



Create a data breach response plan



Leave unused services running on your devices. *Ex. Bluetooth*



Use multi-factor authentication when possible



Plug in random portable devices



Get a cybersecurity insurance policy



Visit insecure websites (Sites without the "S" in HTTPS)

